Send documentation comments to mdsfeedback-doc@cisco.com

Cisco MDS 9000 Family Release Notes for Cisco MDS SAN-OS Release 1.1(2)

CCO Date: July 30, 2003

Text Part Number: OL-4376-03 A0

This document describes the caveats and limitations for switches in the Cisco MDS 9000 Family. Use this document in conjunction with documents listed in the "Related Documentation" section on page 14.

Note Release notes are sometimes updated with new information on restrictions and caveats. Refer to the following website for the most recent version of the *Cisco MDS 9000 Family Release Notes*: http://www.cisco.com/en/US/products/hw/ps4159/ps4358/prod_release_notes_list.html

Table 1 shows the on-line change history for this document.

Table 1 On-Line History Change

Revision	Date	Description
A0	06/23/2005	Added DDTS CSCei25319

Contents

This document includes the following section:

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco MDS 9000 Family of multilayer directors and fabric switches offer intelligent fabric-switching services that realize maximum performance while ensuring high reliability levels. They combine robust and flexible hardware architecture with multiple layers of network and storage management intelligence. This powerful combination enables highly available, scalable storage networks that provide advanced security and unified management features.

The Cisco MDS 9000 Family provides intelligent networking features such as multiprotocol and multitransport integration, virtual SANs (VSANs), advanced security, sophisticated debug analysis tools, and unified SAN management.

System Requirements

This section describes the system requirements for Cisco MDS SAN-OS Release 1.1(2) and includes the following topics:

Hardware Supported

Table 2 lists the hardware components supported on the Cisco MDS 9000 Family and the minimum software version required. See the "Determining the Software Version" section on page 4.

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Applicable Products
Software	M95S1K9-1.1.2	MDS 9500 Series supervisor/fabric-I, enterprise software	MDS 9500 Series only
	M92S1K9-1.1.2	MDS 9216 enterprise software	MDS 9216 only
Chassis	DS-C9509	MDS 9509 director, base configuration (9-slot modular chassis includes 7 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately)	MDS 9509 only
	DS-C9506	MDS 9506 director (6-slot modular chassis includes 4 slots for switching modules and 2 slots for supervisor modules—SFPs sold separately.	MDS 9506 only
	DS-C9216-K9	MDS 9216 16-port semi-modular fabric switch (includes sixteen 1 / 2-Gbps Fibre Channel ports, power supply, and expansion slot—SFPs sold separately)	MDS 9216 only
Supervisor modules	DS-X9530-SF1-K9	MDS 9500 supervisor/fabric-I, module	MDS 9500 Series only

Table 2 Cisco MDS 9000 Family Supported Hardware Modules and Minimum Software Requirements

Component	Part Number	Description	Applicable Products
Switching modules	DS-X9016	MDS 9000 16-port 2/1-Gbps Fibre Channel module (SFPs sold separately)	MDS 9500 Series and 9216
	DS-X9032	MDS 9000 32-port 2/1-Gbps Fibre Channel module (SFPs sold separately)	
Services modules	DS-X9308-SMIP	An eight-port (8) Gigabit Ethernet IP storage services module.	
LC-type fiber-optic SFP[1]	DS-SFP-FC-2G-SW	2/1-Gbps Fibre Channel — short wave SFP	MDS 9000 Family
	DS-SFP-FC-2G-LW	2/1-Gbps Fibre Channel — long wave SFP	
	DS-SFP-FCGE-SW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel—short wave SFP	
	DS-SFP-FCGE-LW	1-Gbps Ethernet and 2/1-Gbps Fibre Channel — long wave SFP	
CWDM[2]	CWDM-SFP-xxxx-2G	Gigabit Ethernet and 2/1-Gbps Fibre Channel SFP LC interface xxxx nm, where xxxx = 1470, 1490, 1510, 1530, 1550, 1570, 1590, or 1610 nm	MDS 9500 Series and 9216
	CWDM-MUX-4	Add/drop multiplexer for four CWDM wavelengths	
	CWDM-MUX-8	Add/drop multiplexer for eight CWDM wavelengths	
	CWDM-CHASSIS-2	Two slot chassis for CWDM add/drop multiplexer(s)	
Power supplies	DS-CAC-845W	845W[3] AC power supply for MDS 9216	MDS 9216 only
	DS-CAC-2500W	2500W AC power supply	MDS 9509 only
	DS-CDC-2500W	2500W DC power supply	
	DS-CAC-4000W-US	4000W AC power supply for US (cable attached)	
	DS-CAC-4000W-INT	4000W AC power supply international (cable attached)	
	DS-CAC-1900W	1900W AC power supply for MDS 9506	MDS 9506 only
	DS-CDC-1900W	1900W DC power supply for MDS 9506	
CompactFlash	MEM-MDS-FLD512M	MDS 9500 supervisor CompactFlash disk, 512MB	MDS 9500 Series only
Port analyzer adapter	DS-PAA	A standalone Fibre Channel-to-Ethernet adapter that allows for simple, transparent analysis of Fibre Channel traffic in a switched fabric.	MDS 9000 Family

1. SFP = small form factor pluggable
2. CWDM = coarse wave division multiplexing
3. W = Watt

Determining the Software Version

Note We strongly recommend that you use the latest available software release for all Cisco MDS 9000 Family products.

To determine the version of the Cisco SAN-OS software currently running on a Cisco MDS 9000 Family switch, log in to the switch and enter the **show version** EXEC command.

Feature Set

This Cisco MDS SAN-OS Release 1.1(2) software is packaged in feature sets (also called software images) depending on the platform. The Cisco MDS SAN-OS software feature sets available for the Cisco MDS 9000 Family include Ethernet, Fibre Channel (1 Gbps and 2 Gbps), SNMP, and IP packets.

Image Upgrade Matrix

Table 3 lists the image upgrade (and downgrade) options for Cisco MDS SAN-OS Release 1.1(2).

Table 3 Cisco MDS SAN-OS Release 1.1(2) Image Upgrade/Downgrade Matrix

Upgrade To Release 1.1(2) From	Non-Disruptive
Release 1.1(1a)	Yes
Release 1.0(5)	Yes
Release 1.0(4)	Yes
Release 1.0(3a)	Yes
Release 1.0(2a)	No
Downgrade From Release 1.1(2) To	**Non-Disruptive**
Release 1.1(1a)	Yes
Release 1.0(5)	Yes
Release 1.0(4)	Yes
Release 1.0(3a)	Yes
Release 1.0(2a)	No

New Features in Release 1.1(2)

SAN-OS Release 1.1(2) is a maintenance release for switches in the Cisco MDS 9000 Family. See the "Caveats" section on page 8 for details on closed and outstanding caveats and limitations.

Note The *Release Notes* are specific to this maintenance release. For the rest of the 1.1(2) documentation, refer to the Release 1.1(1a) document set (see the "Related Documentation" section on page 14).

Configuring Performance Buffers

Regardless of the configured Rx BB_credit value, you can manually configure the performance buffer value for specific applications (for example, forwarding frames over FCIP interfaces).

For each physical Fibre Channel interface in any switch in the Cisco MDS 9000 Family, you can specify the amount of performance buffers allocated in addition to the configured receive BB_credit value.

Refer to Cisco MDS 9000 Family Configuration Guide, Release 1.2(1a) for details on this feature.

The show tech support Command

The **show tech-support** command is useful when collecting a large amount of information about your switch for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

The **show tech-support** command displays the output of several **show** commands at once. The output from this command will vary depending on your configuration. Use the **show tech-support** command in EXEC mode to display general information about the switch when reporting a problem.

You can choose to have detailed information for each command or even specify the output for a particular interface, module or VSAN. Each command output is separated by line and the command precedes the output.

This command was available in Release 1.1(1a) and modified in Release 1.1(2).

Limitations and Restrictions

The following limitations and restrictions apply to all switches in the Cisco MDS 9000 Family:

- "Downgrading from a Higher Release" section on page 7
- "Compatible iSCSI Drivers" section on page 8
- "Restoring the Configured Redundancy Mode" section on page 7
- Compatible iSCSI Drivers, page 8
- Caveats Resolved in Release 1.1(2), page 8
- Resolved Caveats, page 10
- Open Caveats, page 12

Downgrading from a Higher Release

When downgrading any switch in the Cisco MDS 9000 Family, avoid using the **reload** command:

Tip Use the **install all** command to gracefully reload the switch and handle configuration conversions.

For example, to revert to Release 1.0(4) or 1.0(3a) from Release 1.x, follow these steps:

Step 1 Save the configuration using the **copy running-config startup-config** command to save the new configuration into nonvolatile storage.

Step 2 Issue the **install all** command to reload the switch.

Refer to the *Cisco MDS 9000 Family Configuration Guide* for further information.

Restoring the Configured Redundancy Mode

Tip If you have configured the **combined** mode as the redundancy mode for power supplies on a Cisco MDS 9509 switch, exert care when using the sequence of the **write erase** and **reload** commands before rolling back to a saved configuration.

As a result of issuing the **write erase** command and the **reload** command, you restore the switch settings to its factory defaults. This sequence also restores the redundancy mode setting for the power supplies back to the **redundant** mode (default).

Depending on the types of power supplies, the input voltage, and the number of modules (line cards) in the chassis, the redundancy mode may prevent the line cards from being powered on after a system reboot.

If you use this sequence, the commands that apply to the powered down line cards will not be enforced on the switch (and will not be part of its running configuration).

When using the sequence of the **write erase** and **reload** commands before rolling back to a saved configuration, follow these steps:

Step 1 Manually change the **redundant** mode configuration to **combined** mode, if originally configured as such.

Step 2 Wait until all modules are back online—the module status displays `ok` in response to the **show module** command.

Step 3 Rollback to the saved configuration using the **copy** command.

Compatible iSCSI Drivers

Each iSCSI host that requires access to storage via the IPS module needs to have a compatible iSCSI driver installed.

The CCO website at http://www.cisco.com/kobayashi/sw-center/sw-stornet.shtml provides a list of compatible drivers.

Caveats Resolved in Release 1.1(2)

The following caveats were resolved in Release 1.1(2):

- CSCeb83751
- CSCeb24370
- CSCeb18262
- CSCeb50783
- CSCeb26940
- CSCeb25354
- CSCeb42054
- CSCeb10177
- CSCeb17094
- CSCeb19764
- CSCeb26498
- CSCeb36758
- CSCeb29307
- CSCeb28919
- CSCeb28812
- CSCeb45606

Caveats

This section lists the caveats and corrected caveats for this release. Use Table 4 to determine the status of a particular caveat. In the table, “R” indicates a resolved caveat, and “O” indicates an open caveat.

Table 4 Release Caveats and Caveats Corrected Reference

	Software Release (Resolved or Open)	
DDTS Number	1.1.(1a)	1.1(2)
Severity 1		
CSCeb83751		R
CSCeb24370		R
Severity 2		

Table 4 Release Caveats and Caveats Corrected Reference

	Software Release (Resolved or Open)	
DDTS Number	**1.1.(1a)**	**1.1(2)**
CSCeb18262	O	R
CSCeb50783		R
CSCeb26940		R
CSCeb25354		R
CSCdz31332	O	O
CSCeb01264	O	O
CSCeb05095	O	O
CSCeb16270	O	O
CSCei25319	O	O
Severity 3		
CSCeb42054	O	R
CSCeb10177	O	R
CSCeb17094	O	R
CSCeb19764		R
CSCeb26498		R
CSCeb36758		R
CSCeb29307		R
CSCeb28919		R
CSCeb28812		R
CSCeb45606		R
CSCeb01112	O	O
CSCdz12179	O	O
CSCdz43707	O	O
CSCea60652	O	O
CSCeb18066	O	O
CSCea80896	O	O
CSCeb10797	O	O
CSCdz43106	O	O
CSCea45726	O	O
CSCea82028	O	O
CSCeb19609	O	O
CSCeb19588	O	O
CSCeb34865	O	O
CSCeb74526	O	O
CSCeg61535	O	O

Resolved Caveats

- CSCeb83751

  Symptom: A Cisco MDS 9500 director, with 16-port modules currently running version 1.1(2), 1.1(3), or 1.2(1A), that was non-disruptively upgraded from version 1.0(x), 1.1(1), or 1.1(1A) and then encountered a link reinitialization on one of the 16 ports can cause the system to get into an unpredictable state and may require a switch reset to recover.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb83751

- CSCeb24370

  Symptom: Displaying the name server database for a range of VSANs only works if the name server contains entries for all the VSANs in the range.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb24370

- CSCeb18262

  Symptom: After issuing the **fcdomain manager restart disruptive** command, an IBM tape 3590 port on the switch displays a `not connected` status.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb18262

- CSCeb50783

  Symptom: When a private loop device connects to a TL port that is in the up state, fabric devices that are in the same VSAN and zone as the newly inserted loop devices receive multiple proxies for each loop device instead of just one.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb50783

- CSCeb26940

  Symptom: When you delete roles, they reappear after the switch is rebooted.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb26940

- CSCeb25354

  Symptom: Removing and inserting a standby supervisor causes it to fail the boot procedure (at the boot loader prompt). No alert or notification is generated.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb25354

- CSCeb42054

  Symptom: During switch bootup, occasionally some modules may fail to come online. The following messages are reported:

  - `XBAR-2-MOD_CONNECTION_FAILURE: Xbar connection with module x failed`
  - `XBAR-1-XBAR_ASIC_FATAL_ERROR: Encountered Fatal ASIC Error for module x device 12 error 0xc02message`

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb42054

- CSCeb10177

  Symptom: Issuing a **show switchover impact** command while any module is booting up can cause the switch to failover to the standby supervisor.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb10177

- CSCeb17094

  Symptom: The following IPS module port configurations are not allowed:

  - If a member port has subinterfaces, then the member port cannot be added to any PortChannel.
  - If a member port is part of a PortChannel, then you cannot create subinterfaces in this member port.
  - If a Gigabit Ethernet port is part of a PortChannel, then you cannot create a different PortChannel on its adjacent port.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb17094

- CSCeb19764

  Symptom: When fabrics are merged by bringing up an inter-switch link, the active Zone Set name in every switch is different based on the local switch configuration.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb17094

- CSCeb26498

  Symptom: The **show fcs database** command returns entries with 0.0.0.0 as the IP address.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb26498

- CSCeb36758

  Symptom: When a link is brought up, the following error message is generated:

  ```
  Error in processing LSA packet on intf fc_/_ VSAN _, Error = Illegal state.
  ```

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb36758

- CSCeb29307

  Symptom: When a power supply that is turned off while a switch is running, the Device Manager does not display the power supply.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb29307

- CSCeb28919

  Symptom: A SNMP trunk VSAN trap is not generated for each VSAN of a trunking PortChannel, when a member port goes down. Also when a trunk member port comes up, the SNMP VSAN traps are generated for each VSAN, but they have incorrect trunk operational port status.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb28919

- CSCeb28812

  Symptom: When a power supply that is turned on or off, the corresponding SNMP trap displays an incorrect AdminStatus.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb28812

- CSCeb45606

  Symptom: Issuing a **show hardware** command displays the same serial number for both active and standby supervisors.

  Please use the following URL for further information:
  http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCeb45606

Open Caveats

- CSCdz31332

  Symptom: If automatic image synchronization is enabled, and the standby supervisor module is synchronizing the image from the active supervisor, the switch will not stop you from issuing the **reload** command on the active or standby supervisor modules. This may result in a failure to synchronize the images.

  Workaround: Be sure to allow sufficient time for the images to be synchronized before reloading a supervisor module. Use the **show system status redundancy** CLI command to check the standby supervisor status.

- CSCeb01264

  Symptom: When you issue the **copy startup-config running-config** command on a switch which is already up and running, the trunking ports may flap, due to reapplication of allowed VSANs for trunking ports in the startup configuration.

  Workaround: Ensure that the startup configuration does not contain any allowed VSAN configuration for trunking ports (trunking ports default to the allowed VSAN configuration).

- CSCeb05095

  Symptom: If a **copy running-config startup-config** command is issued when a switching module is temporarily down, the configuration for that module will be deleted from the system. This primarily occurs at boot time before all the modules are online.

  Workaround: First issue the **show module** command to ensure that all modules are online before issuing a **copy running-config startup-config** command.

- CSCeb16270

  Symptom: Avoid using the same TCP port number for iSCSI and FCIP protocols on an IP Storage Services module (IPS module) port.

  Workaround: None

- CSCei25319

  Sympton: An error message in the log file occurs because the platform manager component passes the wrong parameter while responding to a SNMP query. In some cases, this results in the query not being responded to.

  Workaround: Perform a refresh on Device Manager to clear the problem.

- CSCeb01112

Symptom: Importing the ASCII configuration multiple times in the same switch can cause the FCIP interface to go into `error disabled` state.

Workaround: None.

- CSCdz12179

  Symptom: When the Fabric Manager or Device Manager communicates with the Cisco MDS switch through Virtual Private Network (VPN) or any Network Address Translation (NAT) scheme, a generic error message occurs while adding duplicate zone members from a VPN connection.

  Workaround: None. If an error occurs while running through VPN/NAT, all errors will show up as generic errors without a detailed message describing the error.

- CSCdz43707

  Symptom: The Fabric Manager or Device Manager reports an error for all operations if the switch is multihomed (both IPFC-based in-band management and the out-of-band management interface are up) and the Fabric or Device Manager was started using the IPFC address. Typically, you will see a `notInTime window` error in the Device Manager and all SNMP set operations fail.

  Workaround: If the switch is multihomed, then start the Fabric or Device Manager on the switch using the out-of-band management interface IP address.

- CSCea60652

  Symptom: For iSCSI configurations, both **no pwwn** *hh:hh:hh:hh:hh:hh:hh:hh* and **no pwwn auto** *number* delete all the pWWNs for a given target.

  Workaround: None.

- CSCeb18066

  Symptom: If you change the iSCSI switchport identification from name to IP address, the TCP sessions are not terminated.

  Workaround: None.

- CSCea80896

  Symptom: The Fabric Manager and Device Manager do not support iSCSI TCP parameter configuration and display.

  Workaround: None.

- CSCeb10797

  Symptom: When you delete a pWWN for an auto-created iSCSI initiator using the Device Manager, (removed from snmp fcAddress table), it still shows up in the CLI (the initiator is still auto-created).

  Workaround: None.

- CSCdz43106

  Symptom: The counter values freeze if the Device Manager port monitor window has been up and running for a long time (overnight or a few days).

  Workaround: Close the frozen Device Manager window and re-open Device Manager.

- CSCea45726

  Symptom: The Device Manager shows a port in the down state (red square) when the operational status of the port is up. This rare occurrence is due to the failure cause of the port not being empty (for example, the failure case reflects the `initializing` state).

  Workaround: None.

- CSCea82028

  Symptom: When a switch is upgraded while the Device Manager for that switch is open, a Java error of class cast exception occurs. When this error occurs, some Device Manager menu items are unusable while other menu items remain in this error state.

  Workaround: Close the Device Manager and reopen it.

- CSCeb19609

  Symptom: After plugging and unplugging a Gigabit Ethernet cable multiple times the PortChannel gets isolated and issues a `remote domain manager not responding` error.

  Workaround: None.

- CSCeb19588

  Symptom: Sometimes, the **zone merge import** command results in isolation.

  Workaround: Reissue the command to resolve the isolation problem.

- CSCeb34865

  Symptom: The following error message is issued when you try configuring switch drop latency:

  ```
  changing this parameter is not allowed could not update the value
  ```

  Workaround: None. Switch drop latency is not configurable in this release of the software.

- CSCeb74526

  Symptom: SNMP timeouts occur, or you have difficulty logging into a switch. This can happen if there are two NICs in the same host, and the Java environment attempts to access a switch through the incorrect NIC.

  Workaround: Open the Windows shortcuts to Fabric Manager and Device Manager. Add the following parameter to the shortcut, after **java.exe"**:

  -Dmds.nmsAddress=*nic IP address to use*

  Below is an example of what the full line might look like for Fabric Manager:

  "C:\Program Files\Java\j2re1.4.1\bin\javaw.exe" **-Dmds.nmsAddress=192.168.0.1** -Dsun.java2d.ddoffscreen=false -cp bitmaps.jar;sm.jar;dm.jar;dmdb.jar;dmhelp.jar; esper.jar;layout.jar;jchart.jar;jh.jar;jnm.jar;sanmgr-topo.jar;snmp.jar;agent.jar -Xms6m com.andiamo.sm.SM

- CSCeg61535

  Symptom:The Telnet server may not be disabled even if you disable it through setup. A telnet session will still work in the switch.

  Workaround: Issue the **no telnet server enable** command in configuration mode to disable telnet after you login to the switch.

Related Documentation

Regulatory Compliance and Safety Information for the Cisco MDS 9000 Family

Cisco MDS 9100 Series Quick Start Guide

Cisco MDS 9500 Series and Cisco MDS 9216 Quick Start Guide

Cisco MDS 9100 Series Hardware Installation Guide

Cisco MDS 9216 Switch Hardware Installation Guide

Cisco MDS 9500 Series Hardware Installation Guide

Cisco MDS 9000 Family Command Reference

Cisco MDS 9000 Family Configuration Guide

Cisco MDS 9000 Family Fabric Manager User Guide

Cisco MDS 9000 Family Troubleshooting Guide

Cisco MDS 9000 Family System Messages Guide

Cisco MDS 9000 Family MIB Reference Guide

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to mdsfeedback-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Note If you purchased this product through a Cisco reseller, contact the reseller directly for technical support. If you purchased this product directly from Cisco, contact Cisco Technical Support at this URL: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

- Priority level 1 (P1)—An existing network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html